Attorney Docket No. 1538.1040

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Ikuo MIKITA

Application No.: Group Art Unit:

Filed: September 11, 2003 Examiner:

For: ACCESS CONTROL TECHNIQUE USING CRYPTOGRAPHIC TECHNOLOGY

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-269115

Filed: September 13, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 11, 2003 By: _____
J. Randall Beckers
Registration No. 30,358

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月１３日

出願番号
Application Number: 特願２００２－２６９１１５

[ST. 10/C]: ［ＪＰ２００２－２６９１１５］

出願人
Applicant(s): 富士通株式会社

２００３年　７月２４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５８９２９

【書類名】　特許願
【整理番号】　0252179
【提出日】　平成14年 9月13日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明の名称】　センタ・システムにおける情報処理方法及びアクセス権限管理方法
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　蒔田　育生
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100103528
【弁理士】
【氏名又は名称】　原田　一男
【電話番号】　045-290-2761
【手数料の表示】
【予納台帳番号】　076762
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9909129
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　センタ・システムにおける情報処理方法及びアクセス権限管理方法

【特許請求の範囲】

【請求項１】

特定のデータに対する第１の電子署名と前記特定のデータの閲覧が許可されるべき第１のユーザのデータとを第２のユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記第２のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

を含むセンタ・システムにおける情報処理方法。

【請求項２】

前記閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前記第２のユーザの端末に送信するステップ

を含むことを特徴とする請求項１記載のセンタ・システムにおける情報処理方法。

【請求項３】

特定のデータに対する第１の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

を含むセンタ・システムにおけるアクセス権限管理方法。

【請求項４】

前記第１の電子署名と前記第２の電子署名とが一致しないと判断された場合には、前記第１の電子署名から第１のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第１のハッシュ・データと前記特定のデータに対応してデータ登録部に登録された第２のハッシュ・データとを比較するステップと、

前記第１のハッシュ・データと前記第２のハッシュ・データとが一致すると判断された場合には、前記ユーザに対して前記特定のデータの閲覧権限を付与する設定を行うステップと、

をさらに含む請求項３記載のセンタ・システムにおけるアクセス権限管理方法。

【請求項５】

前記第１のハッシュ・データと前記第２のハッシュ・データとが一致しないと判断された場合には、前記ユーザの端末にアクセス拒否通知を送信するステップ

をさらに含む請求項４記載のセンタ・システムにおけるアクセス権限管理方法。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、暗号技術を用いたアクセス制御技術に関する。

【０００２】

【従来の技術】

従来、データベースなどにおいてユーザのアクセス権限を管理する場合には、各レコード又はレコード群に対してアクセスポリシーを記述するデータを登録しておき、ユーザからアクセスがあった場合には、当該アクセスポリシーを記述するデータに基づき、ユーザに対して参照、更新などを許可するような技術が一般的であった。一方暗号技術は、一般に２以上のユーザ間の通信の秘匿や電子署名を用いた改竄の有無の確認などに用いられていた。なお、一般的な技術としては以下のようなものがある。

【０００３】

【特許文献１】

特開２００１－４４９８８号公報

【特許文献２】

特開２０００－３０６０２６号公報

【０００４】

【発明が解決しようとする課題】

重要なデータをやり取りする場合には、当該重要なデータの暗号化を行い、さらに改竄の有無を確認するため電子署名を添付するといった手法を用いるが、例えばセンタ・システムにおいて重要なデータの管理を行う場合にはさらに当該重要なデータに対する各ユーザのアクセス権限も重要となる。

【０００５】

従って本発明の目的は、暗号化技術を用いたアクセス制御技術を提供することである。

【０００６】

【課題を解決するための手段】

本発明の第１の態様に係る、センタ・システムにおける情報処理方法は、特定のデータに対する第１の電子署名と特定のデータの閲覧が許可されるべき第１のユーザのデータとを第２のユーザの端末から受信し、記憶装置に格納するステップと、受信した第１の電子署名と特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、第１の電子署名と第２の電子署名とが一致すると判断された場合には、第２のユーザによる特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップとを含む。このように特定のデータに対して真正な電子署名を保持しているユーザには、他のユーザに対する閲覧許可権限を付与するものである。

【０００７】

また、上で述べた閲覧可能化ステップが、特定のデータに対応してデータ登録部に登録されたハッシュ・データを第２のユーザの端末に送信するステップを含むような構成とすることも可能である。閲覧可能とされた第２のユーザの端末に

上記特定のデータを直接送信するようにしても良いが、ここではハッシュ・データを第２のユーザの端末に送信する。そして、後に述べるように当該ハッシュ・データから生成される電子署名を含むアクセス要求に応じて、上記特定のデータを閲覧可能か判断し、閲覧可能であれば上記特定のデータを第２のユーザに送信するようにする。

【０００８】

さらに、本発明の第１の態様において、第１の電子署名と第２の電子署名とが一致しないと判断された場合には、第１の電子署名から第２のハッシュ・データを生成し、記憶装置に格納するステップと、第２のハッシュ・データと特定のデータに対応してデータ登録部に登録されたハッシュ・データとを比較するステップと、ハッシュ・データと第２のハッシュ・データとが一致すると判断された場合には、第２のユーザによる特定のデータの閲覧を可能にするための処理を実施する第２閲覧可能化ステップとをさらに含むような構成であってもよい。このように特定のデータに対して真正なハッシュ・データを保持しているユーザには、他のユーザに対する閲覧許可権限を付与するものである。

【０００９】

本発明の第２の態様に係る、センタ・システムにおける情報処理方法は、特定のデータに対する第１の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、受信した第１の電子署名と特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、第１の電子署名と第２の電子署名とが一致すると判断された場合には、ユーザに対して特定のデータの更新権限を付与する設定を行うステップとを含む。

【００１０】

このように特定のデータに対して真正な電子署名を保持しているユーザには、更新権限を付与して、例えば特定のデータを更新可能な態様でユーザの端末に送信したり、更新後のデータの登録を許可する。

【００１１】

また、本発明の第２の態様において、第１の電子署名と前記第２の電子署名とが一致しないと判断された場合には、第１の電子署名から第１のハッシュ・デー

タを生成し、記憶装置に格納するステップと、第１のハッシュ・データと特定のデータに対応してデータ登録部に登録された第２のハッシュ・データとを比較するステップと、第１のハッシュ・データと第２のハッシュ・データとが一致すると判断された場合には、ユーザに対して特定のデータの閲覧権限を付与する設定を行うステップとをさらに含む。このように特定のデータに対して真正なハッシュ・データを保持しているユーザには、閲覧権限を付与して、例えば特定のデータを閲覧のみ可能な態様でユーザの端末に送信する。

【００１２】

さらに、本発明の第２の態様において、第１のハッシュ・データと第２のハッシュ・データとが一致しないと判断された場合には、ユーザの端末にアクセス拒否通知を送信するステップをさらに含むような構成を含むようにしても良い。

【００１３】

本発明の第３の態様に係るセンタ・システムにおけるデータ登録方法は、ユーザの端末から特定のデータを受信した場合、特定のデータのハッシュ・データを生成し、記憶装置に格納するステップと、ユーザの端末にハッシュ・データを送信するステップと、ハッシュ・データから生成される電子署名をユーザの端末から受信し、記憶装置に格納するステップと、特定のデータとハッシュ・データと電子署名とをデータ登録部に登録する登録ステップとを含む。このようにしてデータの登録を実施し、後の利用（閲覧・更新）の準備を行う。

【００１４】

本発明の第４の態様に係るユーザ・システムにおけるデータ・アクセス方法は、ハッシュ記憶部に格納された、特定のデータのハッシュ・データから電子署名を生成し、記憶装置に格納するステップと、電子署名を含むアクセス要求をサーバに送信するステップと、電子署名がサーバに登録されている特定のデータの第２の電子署名と同一である場合には、特定のデータの更新が可能なことを表すデータをサーバから受信し、表示装置に表示するステップとを含む。真正な電子署名を生成できれば、特定のデータの更新が可能となる。

【００１５】

また、電子署名がサーバに登録されている特定のデータの第２の電子署名と同

一ではないが電子署名から生成されるハッシュ・データがサーバに登録されている特定のデータの第２のハッシュ・データと同一である場合には、閲覧のみ可能な態様で特定のデータをサーバから受信し、表示装置に表示するステップをさらに含むような構成であってもよい。電子署名は異なるが、真正なハッシュ・データを保持していれば、特定のデータの参照が可能となる。

【００１６】

なお、本発明に係る情報処理方法、アクセス権限管理方法及びデータ登録方法はプログラム及びコンピュータ・ハードウエアにて実施することができ、このプログラムは、例えばフレキシブルディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。また、ネットワークなどを介して配布される場合もある。尚、中間的な処理結果はメモリに一時保管される。

【００１７】

【発明の実施の形態】

［概要］

例えば貿易業務では、一回の貿易取引で最大２７の企業がトレード・チェインを構成し、４０種類以上の貿易書類が業務プロセスの中で随時作成され、それらが企業間を転々と流通していくという特性がある。例えば、荷主が行う通関依頼プロセスでは、荷主が「インボイス」、「パッキングリスト」を作成し、フォワーダに送付する。更に、フォワーダは「船積通知書」を作成し、荷主に送付する。すなわち、上記プロセス終了時点において、荷主は、貿易書類のうち「インボイス」及び「パッキングリスト」については原本を、「船積通知書」は写しを保持するようになる。また、フォワーダは、「インボイス」及び「パッキングリスト」については写しを、「船積通知書」については原本を保持するようになる。このように、複数の貿易書類を複数企業が作成し、そして同一書類（原本と写し）を複数企業で保有することになる。

【００１８】

このような貿易業務の特性から、共同センタにシステムを設け、当該共同センタにおいて貿易書類を管理する構成を採用する。そして、企業間で実際にやり取

りされるデータを、共同センタ・システムにおいて管理される貿易書類データへのアクセス制御情報とする。以下で説明するように、貿易書類データのハッシュ値（ハッシュ・データとも記す）を、このアクセス制御情報に用いる。また、共同センタ・システムに対しては貿易書類データの電子署名もアクセス制御情報として用いられる。このような構成により、効率的なデータ保管・管理によってシステムリソースを有効利用でき、更に送受信データ量の削減、ネットワーク負荷の軽減と伝送時間の短縮化も実現される。

【００１９】

具体的には、流通している貿易書類データを更新できる権限は、書類作成者のみが有しており、貿易書類データの送付先（更にその先の送付先等を含む）には参照権限のみ付与するものとする。共同センタ・システムで管理する貿易書類データへのアクセス制御を、貿易書類データへの電子署名及びハッシュ値に基づき行うことにより、貿易書類データの更新・参照権限の制御を実現する。これによって、アクセス制御テーブルを使いフラグ等で管理する従来方式に比べて、セキュリティ面で格段の向上を実現できる。また、共同センタのシステムで各貿易書類データのアクセスポリシーを記憶しておく必要がなくなるので、フレキシブルなアクセス制御を可能とする。

【００２０】

［具体的な実施の形態］

図１を用いて本発明の一実施の形態に係るシステム概要を説明する。例えばインターネットなどのネットワーク１には、Ａ社システム３と、共同センタ・システム５と、Ｂ社システム７とが接続されている。ここでは説明の都合上２社のシステムのみ図１に示しているが、多くの企業のシステムがネットワーク１に接続している。

【００２１】

Ａ社システム３は、ウェブ（Ｗｅｂ）ブラウザ機能を保持しており、共同センタ・システム５と暗号化通信を行うことができるようになっている。そして、ハッシュ・データを公開鍵暗号方式における秘密鍵により暗号化し電子署名を生成する電子署名生成部３１と、自らの電子証明書の他例えば共同センタ・システム

５の電子証明書を格納する電子証明書格納部３２と、共同センタ・システム５から受信した貿易書類データのハッシュ・データを格納するハッシュ格納部３３とを有する。

【００２２】

電子証明書格納部３２に格納されるデータの一例を図２（ａ）及び図２（ｂ）に示す。図２（ａ）に示すように電子証明書格納部３２には、保持している本人及び他人の電子証明書の電子証明書発行番号２０１と、電子証明書の所有者情報（例えば所有者名や公開鍵を含む）２０２とが対応付けられて格納されている。また、図２（ｂ）に示すように、本人の電子証明書の電子証明書発行番号２０３と、本人の秘密鍵情報２０４とも対応付けられて格納されている。

【００２３】

ハッシュ格納部３３に格納されるデータの一例を図３に示す。図３に示すようにハッシュ格納部３３には、取引番号（取引識別情報であって、図３（ａ）の例ではＴＲＮ１）毎にフォルダ３０１が設けられており、貿易書類名３０２に対応してハッシュ値３０３が登録されている。図３の例では、インボイスという貿易書類名に対応して「４４４４４・・・・」というハッシュ値が登録され、パッキングリストという貿易書類名に対応して「３３３３・・・・」というハッシュ値が登録されている。

【００２４】

Ｂ社システム７は、Ｗｅｂブラウザ機能を保持しており、共同センタ・システム５と暗号化通信を行うことができるようになっている。そして、ハッシュ・データを公開鍵暗号方式における秘密鍵により暗号化し電子署名を生成する電子署名生成部７１と、自らの電子証明書の他例えば共同センタ・システム５の電子証明書を格納する電子証明書格納部７２と、共同センタ・システム５から受信した貿易書類データのハッシュ・データを格納するハッシュ格納部７３とを有する。電子証明書格納部７２に格納されるデータ形式は図２（ａ）及び図２（ｂ）に示したものと同様である。ハッシュ格納部７３に格納されるデータ形式は図３に示したものと同様である。

【００２５】

共同センタ・システム５は、Ｗｅｂサーバ機能を保持しており、Ａ社システム３やＢ社システム７と暗号化通信を行うことができるようになっている。そして、貿易書類処理部５１と、貿易書類ファイルから所定のハッシュ関数に従ってハッシュ・データを生成するハッシュ生成部５２と、電子署名及びハッシュの照合処理などを実施する電子署名・ハッシュ処理部５３と、照合処理の結果に基づき貿易書類ファイルへのアクセス制御を実施するアクセス制御部５４と、取引毎に各貿易書類の貿易書類ファイルと電子署名とハッシュ・データとを格納する貿易書類マスタ格納部５５と、共同センタ・システム５の電子証明書とユーザ企業の電子証明書のデータを格納する電子証明書格納部５６と、ユーザ企業との連携処理において用いられるワークエリアである連携作業領域５７とを含む。

【００２６】

貿易書類処理部５１は、貿易書類作成者のシステムから貿易書類データを受信して貿易書類ファイルを生成し、連携作業領域５７に格納したり、貿易書類マスタ格納部５５に登録したり、アクセスが許可された場合には貿易書類マスタ格納部５５に格納された貿易書類ファイルを適切な表示形態のデータに変換するといった処理を実施する。

【００２７】

貿易書類マスタ格納部５５に格納されるデータの一例を図４（ａ）、図４（ｂ）及び図４（ｃ）に示す。図４（ａ）に示すように貿易書類マスタ格納部５５には、取引番号（取引識別情報であって、図４（ａ）の例ではＴＲＮ１）毎にフォルダ４０１が設けられており、貿易書類名４０２に対応して貿易書類の属性情報と内容４０３が登録されている。また、図４（ｂ）に示すように、取引番号毎に設けられたフォルダ４０１には、貿易書類名４０２に対応して電子署名４０６も登録されている。さらに、図４（ｃ）に示すように、取引番号毎に設けられたフォルダ４０１には、貿易書類名４０２に対応してハッシュ値４０９も登録されている。

【００２８】

これをファイル構成図として示せば図５に示されたような状態となる。図５の例では、取引番号毎にフォルダ４０１が設けられ、当該取引に関連する貿易書類

ファイルであるインボイス・ファイル５１１と、インボイス・ファイル５１１の電子署名５１２と、インボイス・ファイル５１１のハッシュ値５１３と、当該取引に関連する貿易書類ファイルであるパッキングリスト・ファイル５１４と、パッキングリスト・ファイル５１４の電子署名５１５と、パッキングリスト・ファイル５１４のハッシュ値５１６とが含まれる。

【００２９】

なお、電子証明書格納部５６に格納されるデータ形式は、図２（ａ）及び図２（ｂ）に示したものと同様である。また、連携作業領域５７は、Ａ社用領域５７１、Ｂ社用領域５７２など各社用の領域が設けられる。

【００３０】

次に図６乃至図１１を用いて図１に示したシステムの動作について説明する。なお、以下の説明では、各システム間の通信は原則として暗号化されており、各ステップにおいては暗号・検証についての説明は省略するものとする。また、Ａ社及びＢ社は共同センタの電子証明書を保持しており、共同センタはＡ社及びＢ社の電子証明書を保持しているものとする。場合によっては、通信の都度に自己の電子証明書を添付して送信するような場合もある。

【００３１】

図６を用いて、貿易書類データの登録処理を説明する。なお、Ａ社が貿易書類を作成するものとする。Ａ社システム３は、例えば共同センタ・システム５から受信した貿易書類データ登録ページを表示装置に表示し、Ａ社システム３のユーザにデータ入力欄にデータを入力するように促す。Ａ社システム３のユーザが、データ入力欄にデータを入力し、データの送信を指示すると、Ａ社システム３は入力された貿易書類データを共同センタ・システム５に送信する（ステップＳ１）。共同センタ・システム５は、Ａ社システム３から貿易書類データを受信すると（ステップＳ３）、貿易書類処理部５１は貿易書類データから貿易書類ファイルを生成し、連携作業領域５７のＡ社用領域５７１に格納する（ステップＳ５）。次にハッシュ生成部５２は、連携作業領域５７のＡ社用領域５７１に格納された貿易書類ファイルのハッシュ値を計算し、また連携作業領域５７のＡ社用領域５７１にハッシュ値を格納する（ステップＳ７）。

【００３２】

ハッシュ値が計算されると、共同センタ・システム５は、ハッシュ値のダウンロード要求をＡ社システム３に送信する（ステップＳ９）。Ａ社システム３は、ハッシュ値のダウンロード要求を受信し、表示装置に表示する（ステップＳ１１）。この表示に応じて、Ａ社システム３のユーザがダウンロード指示を入力すると、Ａ社システム３は、ハッシュ値のダウンロード要求を共同センタ・システム５に送信する（ステップＳ１３）。共同センタ・システム５は、Ａ社システム３からハッシュ値のダウンロード要求を受信すると（ステップＳ１５）、連携作業領域５７のＡ社用領域５７１からハッシュ値を読み出して、取引番号及び貿易書類名の情報と共にＡ社システム３に送信する（ステップＳ１７）。Ａ社システム３は、共同センタ・システム５から取引番号及び貿易書類名の情報と共にハッシュ値を受信すると、ハッシュ格納部３３における取引番号のフォルダ内に貿易書類名に対応して登録する（ステップＳ１９）。なお、取引番号のフォルダが生成されていないければ、このステップにおいて生成する。

【００３３】

次に、Ａ社システム３の電子署名生成部３１は、受信したハッシュ値を電子証明書格納部３２に格納された自らの秘密鍵で暗号化し、電子署名を生成する（ステップＳ２１）。電子署名は、テンポラリの電子署名格納部に格納される。例えば図７に示すように取引番号のフォルダ７０１が設けられ、貿易書類名７０２に対応して生成された電子署名７０３が登録される。そして、Ａ社システム３は、共同センタ・システム５に生成した電子署名を取引番号及び貿易書類名の情報と共に送信する（ステップＳ２３）。なお、生成した電子署名については、送信が完了した時点で盗用防止等のために消去するものとする。

【００３４】

共同センタ・システム５は、Ａ社システム３から取引番号及び貿易書類名の情報と共に電子署名を受信し（ステップＳ２５）、電子署名・ハッシュ処理部５３は、受信した電子署名の確認処理を実施する（ステップＳ２７）。電子署名を電子証明書格納部５６に格納されたＡ社の公開鍵で復号化してハッシュ値を生成し、連携作業領域５７のＡ社用領域５７１に格納された対応ハッシュ値と比較する

。両ハッシュ値が一致していれば真正な電子署名を受信したことになるため、貿易書類処理部５１は、連携作業領域５７のＡ社用領域５７１に格納された貿易書類ファイル及びハッシュ値、並びに受信した電子署名を貿易書類マスタ格納部５５の取引番号フォルダに登録する（ステップＳ２９）。そして、連携作業領域５７のＡ社用領域５７１をクリアする（ステップＳ３１）。受信した電子署名に対応する貿易書類ファイル及びハッシュ値を消去するものである。

【００３５】

以上のようにすれば、貿易書類データの登録と共に、ハッシュ値及び電子署名を共同センタ・システム５に登録することができる。なお、ハッシュ値を共同センタ・システム５において生成するため、ハッシュ値を元に検証処理を行うことができ、適切な電子署名が貿易書類ファイルに対応して登録されることを保証できる。

【００３６】

次に図８及び図９を用いてＡ社がＢ社への貿易書類の送付を共同センタ・システム５に依頼する際の処理を説明する。Ａ社システム３の電子署名生成部３１は、例えばＡ社システム３のユーザにより送信すべき貿易書類の取引番号と貿易書類名と送付先とが指定されると、送信すべき貿易書類ファイルのハッシュ値をハッシュ格納部３３から読み出し、電子証明書格納部３２に格納されたＡ社の秘密鍵でハッシュ値を暗号化し、電子署名を生成する（ステップＳ４１）。電子署名は、図７に示すようなテンポラリの電子署名格納部に格納される。そして、Ａ社システム３は、送付先データと取引番号と貿易書類名と電子署名とを共同センタ・システム５に送信する（ステップＳ４３）。例えば図９にステップＳ４３において送信される電文形式の一例を示す。図９の例では、共同センタ・システム５のアドレスである宛先データ９０１と、例えば送信先企業ＩＤである送信先企業データ９０２と、例えば送信元企業ＩＤである送信元企業データ９０３と、取引番号である取引特定データ９０４と、貿易書類名（１）９０５と、貿易書類ファイルの電子署名（１）９０６と、．．．が含まれる。図９に示されたように一度に何種類かの電子署名を送信することができるようになっている。

【００３７】

共同センタ・システム５は、Ａ社システム３から送付先データと取引番号と貿易書類名と電子署名とを受信し、一旦記憶装置に格納する（ステップＳ４５）。そして、電子署名・ハッシュ処理部５３は、受信した電子署名と、取引番号及び貿易書類名とにより特定され且つ貿易書類マスタ格納部５５に登録された電子署名とを比較し、一致しているか判断する（ステップＳ４７）。もし、両電子署名が同一であると判断された場合には、ステップＳ５５に移行する。Ａ社が貿易書類の作成者であれば、ステップＳ４７からステップＳ５５に移行することになる。一方、両電子署名が同一ではないと判断された場合には、受信した電子署名を、電子証明書格納部５６に格納された送信元企業の公開鍵を用いて復号化することによりハッシュ値を生成し、記憶装置に格納する（ステップＳ４９）。

【００３８】

そして、電子署名・ハッシュ処理部５３は、生成したハッシュ値と、取引番号及び貿易書類名とにより特定され且つ貿易書類マスタ格納部５５に登録されたハッシュ値とを比較し、一致しているか判断する（ステップＳ５１）。もし、両ハッシュ値が同一ではないと判断された場合には、共同センタ・システム５は、エラー通知をＡ社システム３に送信する。Ａ社システム３は、共同センタ・システム５からエラー通知を受信し、表示装置に表示する（ステップＳ５３）。これにより、Ａ社のユーザは、何らかの理由で、貿易書類の指定送付先であるＢ社への送付が許可されなかったことを認識することができる。

【００３９】

一方、両ハッシュ値が同一であると判断された場合及びステップＳ４７において両電子署名が同一であると判断された場合には、貿易書類マスタ格納部５５に登録されている対応ハッシュ値を読み出し、連携作業領域５７の、送付先であるＢ社用領域５７２に格納する（ステップＳ５５）。そして、共同センタ・システム５は、Ｂ社システム７宛にハッシュ値のダウンロード要求を例えば電子メールなどにより送信する（ステップＳ５７）。Ｂ社システム７は、共同センタ・システム５からの、ハッシュ値のダウンロード要求を受信し、表示装置に表示する（ステップＳ５９）。Ｂ社システム７のユーザがハッシュ値のダウンロードを指示すると、Ｂ社システム７はハッシュ値のダウンロード要求を共同センタ・システ

ム５に送信する（ステップＳ６１）。共同センタ・システム５は、Ｂ社システム７からハッシュ値のダウンロード要求を受信すると（ステップＳ６３）、連携作業領域５７のＢ社用領域５７２に格納されているハッシュ値を読み出し、取引番号及び貿易書類名の情報と共にＢ社システム７に送信する（ステップＳ６５）。Ｂ社システム７は、共同センタ・システム５から取引番号及び貿易書類名の情報とハッシュ値とを受信し、ハッシュ格納部７３における取引番号のフォルダに貿易書類名に対応してハッシュ値を登録する（ステップＳ６７）。一方、共同センタ・システム５は、送信が完了すると、連携作業領域５７のＢ社用領域５７２をクリアする（ステップＳ６９）。なお、送信したハッシュ値のみを削除する。

【００４０】

このような処理を実施することにより、適正なハッシュ値を有する企業は、共同センタ・システム５に、他の企業へ貿易書類ファイルのハッシュ値を送付させることができる。なお、本実施の形態では直接貿易書類ファイルを送付先として指定された企業に送付せず、ハッシュ値を送付する。後に説明するようにハッシュ値又は電子署名を用いて参照・更新のアクセス権限を確認の上、アクセス権限に従った形で貿易書類を提示する。これにより、やり取りするデータ量が減少すると共に、セキュリティが高まる。また、適正なハッシュ値を有する企業は貿易書類を作成した企業だけではなく、貿易書類を作成した企業から参照許可を与えられた企業も適正なハッシュ値を有する。従って、適正なハッシュ値を有する企業であれば、他の企業に対して参照許可を与えることができる。すなわち、参照許可を与えられると、当該貿易書類ファイルのハッシュ値を取得することができる。

【００４１】

次に図１０及び図１１を用いて実際にＢ社システム７が貿易書類ファイルにアクセスする際の処理を説明する。Ｂ社のユーザが、アクセスすべき貿易書類の取引番号と貿易書類名とを指定すると、Ｂ社システム７の電子署名生成部７は、ハッシュ格納部７３から該当するハッシュ値を読み出し、電子証明書格納部７２に格納されたＢ社の秘密鍵で暗号化して電子署名を生成し、記憶装置に一旦格納する（ステップＳ７１）。電子署名は、図７に示すようなテンポラリの電子署名格

納部に格納される。そして、Ｂ社システム７は、電子署名と取引番号と貿易書類名とを含むアクセス要求を共同センタ・システム５に送信する（ステップＳ７３）。例えば図１１のようなＢ社システム７から共同センタ・システム５へ送信される。図１１の例では、共同センタ・システム５のアドレスである宛先データ１１０１と、送信元企業ＩＤである送信元企業データ１１０２と、取引番号である取引特定データ１１０３と、貿易書類名（１）１１０４と、貿易書類ファイルの電子署名（１）１１０５と、．．．が含まれる。図１１に示されたように一度に何種類かの電子署名を送信することができるようになっている。

【００４２】

共同センタ・システム５は、Ｂ社システム７から電子署名と取引番号と貿易書類名とを含むアクセス要求を受信すると、一旦記憶装置に格納する（ステップＳ７５）。そして、共同センタ・システム５の電子署名・ハッシュ処理部５３は、貿易書類マスタ格納部５５に登録され且つ取引番号及び貿易書類名により特定される電子署名を読み出し、受信した電子署名と一致するか判断する（ステップＳ７７）。両電子署名が同一である判断された場合、貿易書類の作成者からのアクセスであると認められるので、取引番号及び貿易書類名により指定された貿易書類ファイルへの更新権限が認められる。従って、アクセス制御部５４は、今回のアクセス者に対して取引番号及び貿易書類名により指定された貿易書類ファイルへの更新を許可する設定を行う（ステップＳ９１）。例えば、取引番号及び貿易書類名と今回のアクセス者のＩＤと更新というデータとを、所定期間（例えばログオフするまで）だけ記憶装置に登録しておき、指定された貿易書類ファイルに対する更新要求を許可する。

【００４３】

従って、貿易書類処理部５１は、例えば指定された貿易書類ファイルのデータを修正可能な態様でＢ社システム７に送信する（ステップＳ９３）。例えば、指定された貿易書類ファイルのデータを入力欄に埋め込んだ形のページ・データを生成し、当該ページ・データをＢ社システム７に送信する。Ｂ社システム７は、共同センタ・システム５から、指定された貿易書類ファイルのデータを修正可能な態様で受信し、表示装置に表示する（ステップＳ９５）。この後の処理は、例

えば端子Ａを介して図６の処理に移行し、更新後の貿易書類データに対して貿易書類ファイルを生成して、貿易書類マスタ格納部５５に登録し直すような構成であってもよい。また、差分だけを別ファイルとして貿易書類マスタ格納部５５に登録するような構成であってもよい。

【００４４】

ステップＳ７７において両電子署名が同一ではないと判断された場合、貿易書類の作成者ではない者からのアクセスであると判断される。従って、次に参照を許可された者からのアクセスであるか判断する。電子署名・ハッシュ処理部５３は、電子証明書格納部５６からＢ社の公開鍵を読み出し、電子署名を当該公開鍵で復号化してハッシュ値を生成し、記憶装置に格納する（ステップＳ７９）。そして、電子署名・ハッシュ処理部５３は、貿易書類マスタ格納部５５に登録され且つ取引番号及び取引書類名により特定されるハッシュ値を読み出し、生成したハッシュ値と一致するか判断する（ステップＳ８１）。両ハッシュ値が同一ではないと判断された場合にはアクセスは拒否すべきものであるから、Ｂ社システム７にアクセス不可を表すエラー通知を送信する。Ｂ社システム７は、アクセス不可を表すエラー通知を受信し、表示装置に表示する（ステップＳ８３）。これによりＢ社のユーザは、何らかの理由でアクセスが拒否されたことを認識できる。

【００４５】

一方、両ハッシュ値が一致する場合には、当該貿易書類の参照を許可された者からのアクセスであると認められるので、取引番号及び貿易書類名により指定された貿易書類ファイルへの参照権限が認められる。従って、アクセス制御部５４は、今回のアクセス者に対して取引番号及び貿易書類名により指定された貿易書類ファイルへの参照（閲覧）を許可する設定を行う（ステップＳ８５）。例えば、取引番号及び貿易書類名と今回のアクセス者のＩＤと参照というデータとを、所定期間（例えばログオフするまで）だけ記憶装置に登録しておき、指定された貿易書類ファイルに対する参照要求を許可する。

【００４６】

従って、貿易書類処理部５１は、例えば指定された貿易書類ファイルのデータを参照のみ可能な態様でＢ社システム７に送信する（ステップＳ８７）。例えば

、指定された貿易書類ファイルのデータを表示欄に含む形のページ・データを生成し、当該ページ・データをＢ社システム７に送信する。Ｂ社システム７は、共同センタ・システム５から、指定された貿易書類ファイルのデータを参照のみ可能な態様で受信し、表示装置に表示する（ステップＳ８９）。このようにすれば、Ｂ社のユーザは貿易書類のデータを確認することができる。

【００４７】

以上のような処理を実施することにより、単にハッシュ値を得た者は貿易書類の参照のみ可能であり、貿易書類を生成し且つハッシュ値を有する者は貿易書類の更新が可能となる。ハッシュ値は、様々なユーザに流通することになるが、貿易書類よりはデータ量は少なく、送信データ量を削減させ、記憶容量を減少させることができるようになる。また、ハッシュ値から得られる電子署名をアクセス権限の確認に用いるため、正しい秘密鍵を有する者であることが確認でき、さらに電子署名からハッシュ値を生成する際には適正なユーザであるかも確認できるため、セキュリティも高まっている。また、ハッシュ値を得れば、少なくとも参照のみ可能となるので、アクセス制御のフレキシビリティも高まっている。

【００４８】

以上述べた本発明の一実施の形態は一例であって、本発明はこれに限定されない。すなわち、貿易書類の例で説明したが、アクセス制御の対象たるデータは、貿易書類のデータに限定されず、全てのデータに適用できる。また、図１に示した機能ブロック及びデータ格納部は一例であって、必ずしも実際のプログラム・モジュールとは対応しない場合もある。また、貿易書類マスタ格納部５５におけるデータの管理形態も一例であって、必ずしも取引番号でフォルダを生成する必要は無い。全てのデータに一連の識別情報を付与して、別途データベースで関連を管理する場合もある。共同センタ・システム５へのアクセスは、ログイン後に行う場合もある。

【００４９】

（付記１）

特定のデータに対する第１の電子署名と前記特定のデータの閲覧が許可されるべき第１のユーザのデータとを第２のユーザの端末から受信し、記憶装置に格納

するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記第２のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

を含むセンタ・システムにおける情報処理方法。

【００５０】

（付記２）

前記閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前記第２のユーザの端末に送信するステップ

を含むことを特徴とする付記１記載のセンタ・システムにおける情報処理方法。

【００５１】

（付記３）

前記第１の電子署名と前記第２の電子署名とが一致しないと判断された場合には、前記第１の電子署名から第２のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第２のハッシュ・データと前記特定のデータに対応してデータ登録部に登録されたハッシュ・データとを比較するステップと、

前記ハッシュ・データと前記第２のハッシュ・データとが一致すると判断された場合には、前記第２のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する第２閲覧可能化ステップと、

をさらに含む付記１記載のセンタ・システムにおける情報処理方法。

【００５２】

（付記４）

前記第２閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前

記第２のユーザの端末に送信するステップ

を含むことを特徴とする付記３記載のセンタ・システムにおける情報処理方法。

【００５３】

（付記５）

特定のデータに対する第１の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

を含むセンタ・システムにおけるアクセス権限管理方法。

【００５４】

（付記６）

前記第１の電子署名と前記第２の電子署名とが一致しないと判断された場合には、前記第１の電子署名から第１のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第１のハッシュ・データと前記特定のデータに対応してデータ登録部に登録された第２のハッシュ・データとを比較するステップと、

前記第１のハッシュ・データと前記第２のハッシュ・データとが一致すると判断された場合には、前記ユーザに対して前記特定のデータの閲覧権限を付与する設定を行うステップと、

をさらに含む付記５記載のセンタ・システムにおけるアクセス権限管理方法。

【００５５】

（付記７）

前記第１のハッシュ・データと前記第２のハッシュ・データとが一致しないと判断された場合には、前記ユーザの端末にアクセス拒否通知を送信するステップ

をさらに含む付記６記載のセンタ・システムにおけるアクセス権限管理方法。

【００５６】

（付記８）

前記ユーザの端末から前記特定のデータの更新のためのデータを受信した場合、更新後の前記特定のデータの第３のハッシュ・データを生成し、記憶装置に格納するステップと、

前記ユーザの端末に前記第３のハッシュ・データを送信するステップと、

前記第３のハッシュ・データから生成される第３の電子署名を前記ユーザの端末から受信し、記憶装置に格納するステップと、

更新後の前記特定のデータと前記第３のハッシュ・データと前記第３の電子署名とを前記データ登録部に登録する登録ステップと、

をさらに含む付記５記載のセンタ・システムにおけるアクセス権限管理方法。

【００５７】

（付記９）

前記登録ステップの前に、

前記第３の電子署名から第４のハッシュ・データを生成するステップと、

前記第４のハッシュ・データと前記第３のハッシュ・データとを比較するステップと、

をさらに含み、

前記第４のハッシュ・データと前記第３のハッシュ・データとが一致すると判断された場合に、前記登録ステップを実行する

ことを特徴とする付記８記載のセンタ・システムにおけるアクセス権限管理方法。

【００５８】

（付記１０）

前記ユーザに対して前記特定のデータの閲覧権限が付与された場合、前記ユーザの端末に閲覧のみ可能な態様にて前記特定のデータを送信するステップ、

をさらに含む付記６記載のセンタ・システムにおけるアクセス権限管理方法。

【００５９】

（付記１１）

ユーザの端末から特定のデータを受信した場合、前記特定のデータのハッシュ・データを生成し、記憶装置に格納するステップと、

前記ユーザの端末に前記ハッシュ・データを送信するステップと、

前記ハッシュ・データから生成される電子署名を前記ユーザの端末から受信し、記憶装置に格納するステップと、

前記特定のデータと前記ハッシュ・データと前記電子署名とを前記データ登録部に登録する登録ステップと、

を含むセンタ・システムにおけるデータ登録方法。

【００６０】

（付記１２）

ハッシュ記憶部に格納された、特定のデータのハッシュ・データから電子署名を生成し、記憶装置に格納するステップと、

前記電子署名を含むアクセス要求をサーバに送信するステップと、

前記電子署名が前記サーバに登録されている前記特定のデータの第２の電子署名と同一である場合には、前記特定のデータの更新が可能なことを表すデータを前記サーバから受信し、表示装置に表示するステップと、

を含むユーザ・システムにおけるデータ・アクセス方法。

【００６１】

（付記１３）

前記電子署名が前記サーバに登録されている前記特定のデータの第２の電子署名と同一ではないが前記電子署名から生成されるハッシュ・データが前記サーバに登録されている前記特定のデータの第２のハッシュ・データと同一である場合には、閲覧のみ可能な態様で前記特定のデータを前記サーバから受信し、表示装置に表示するステップと、

を含む付記１２記載のユーザ・システムにおけるデータ・アクセス方法。

【００６２】

（付記１４）

特定のデータに対する第１の電子署名と前記特定のデータの閲覧が許可されるべき第１のユーザのデータとを第２のユーザの端末から受信し、記憶装置に格納

するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記第２のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

をコンピュータに実行させるためのプログラム。

【００６３】

（付記１５）

特定のデータに対する第１の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較するステップと、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

をコンピュータに実行させるためのプログラム。

【００６４】

（付記１６）

付記１４又は１５記載のプログラムを格納する記録媒体。

【００６５】

（付記１７）

特定のデータに対する第１の電子署名と前記特定のデータの閲覧が許可されるべき第１のユーザのデータとを第２のユーザの端末から受信し、記憶装置に格納する手段と、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較する手段と、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記第２のユーザによる前記特定のデータの閲覧を可能にするための処理を実

施する閲覧可能化手段と、

を有する情報処理装置。

【００６６】

（付記１８）

特定のデータに対する第１の電子署名をユーザの端末から受信し、記憶装置に格納する手段と、

受信した前記第１の電子署名と前記特定のデータに対応してデータ登録部に登録された第２の電子署名とを比較する手段と、

前記第１の電子署名と前記第２の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行う手段と、

を有するアクセス権限管理装置。

【００６７】

【発明の効果】

以上述べたように本発明によれば、暗号化技術を用いたアクセス制御技術を提供することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係るシステム概要図である。

【図２】

（ａ）及び（ｂ）は電子証明書格納部に格納されるデータの一例を示す図である。

【図３】

ハッシュ格納部に格納されるデータの一例を示す図である。

【図４】

（ａ）、（ｂ）及び（ｃ）は貿易書類マスタ格納部に格納されるデータの一例を示す図である。

【図５】

ファイル構成の一例を示す図である。

【図６】

貿易書類データの登録処理の処理フローを示す図である。

【図７】

電子署名格納部に格納されるデータの一例を示す図である。

【図８】

貿易書類データ送付のための処理フローを示す図である。

【図９】

貿易書類データの送付のための電文の一例を示す図である。

【図１０】

アクセス権限確認処理のための処理フローを示す図である。

【図１１】

アクセス要求のための電文の一例を示す図である。

【符号の説明】

１　ネットワーク　　３　Ａ社システム

５　共同センタ・システム　　７　Ｂ社システム

３１，７１　電子署名生成部

３２，７２　電子証明書格納部

３３，７３　ハッシュ格納部

５１　貿易書類処理部　　５２　ハッシュ生成部

５３　電子署名・ハッシュ処理部

５４　アクセス制御部

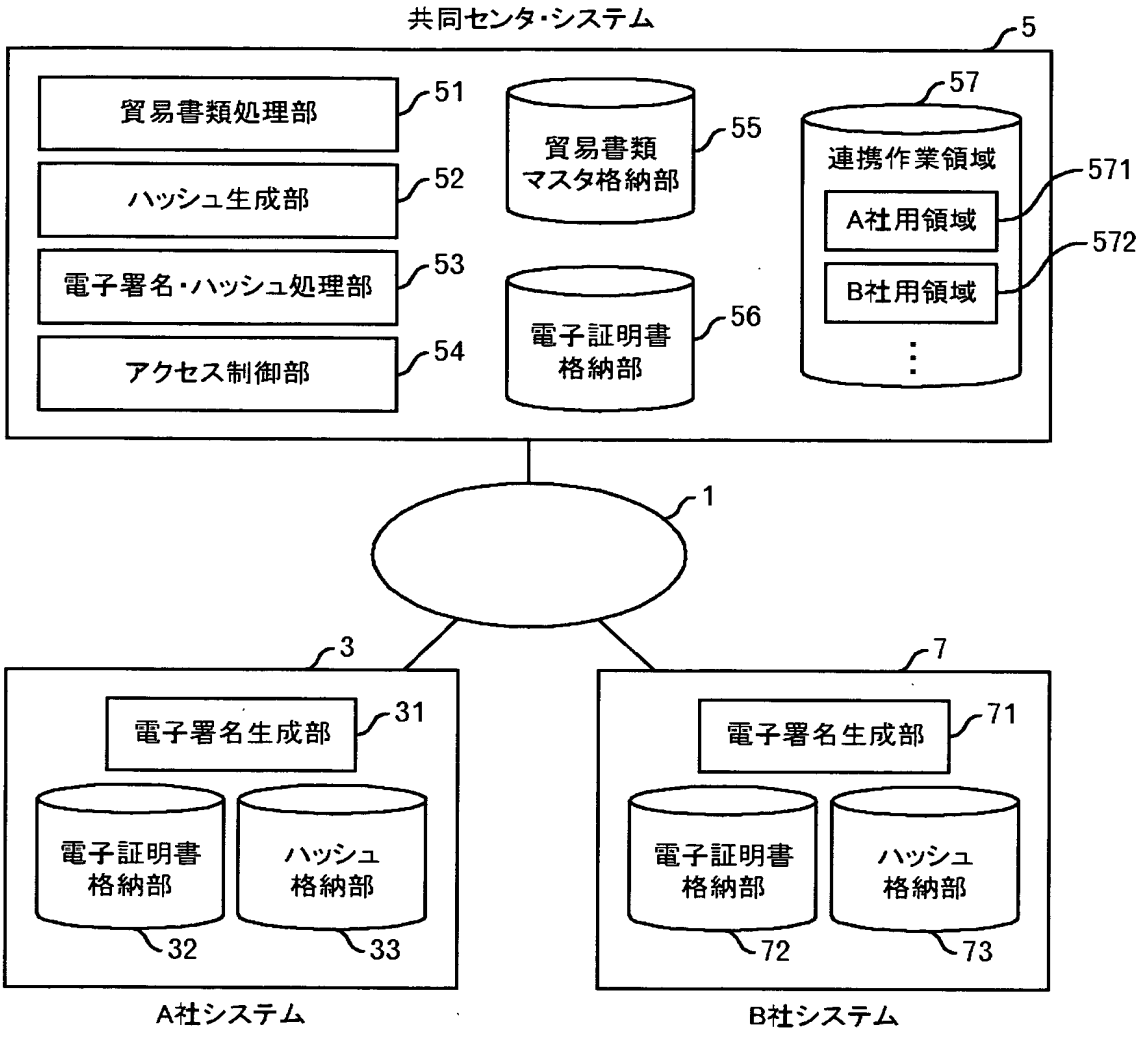
５５　貿易書類マスタ格納部

５６　電子証明書格納部

５７　連携作業領域

【書類名】　　図面

【図１】


共同センタ・システム
5
貿易書類処理部
51
ハッシュ生成部
52
電子署名・ハッシュ処理部
53
アクセス制御部
54
貿易書類
マスタ格納部
55
電子証明書
格納部
56
57
連携作業領域
571
A社用領域
572
B社用領域
1
3
電子署名生成部
31
電子証明書
格納部
32
ハッシュ
格納部
33
A社システム
7
電子署名生成部
71
電子証明書
格納部
72
ハッシュ
格納部
73
B社システム

【図２】

(a)

201 電子証明書発行番号	202 電子証明書所有者情報
A99999999	aaaaa, aaaaaaaa, aaaaaa
ASP99999999	bbbbb, bbbbbbbb, bbbbbb
B99999999	ccccc, cccccccc, cccccc
⋮	⋮

(b)

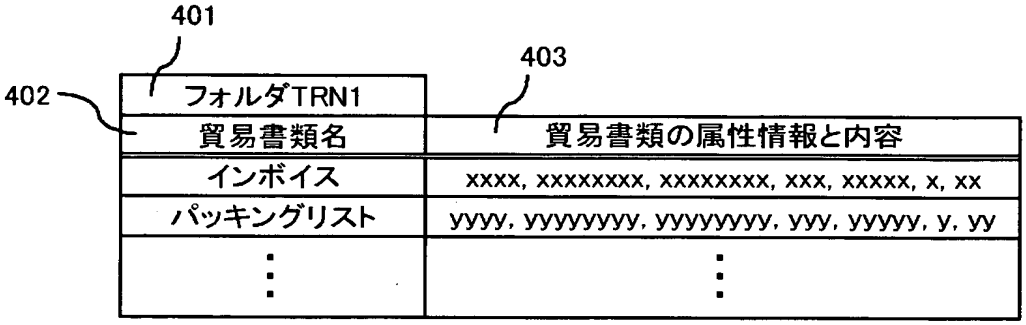
203 電子証明書発行番号	204 秘密鍵情報
A99999999	0101010101・・・

【図３】

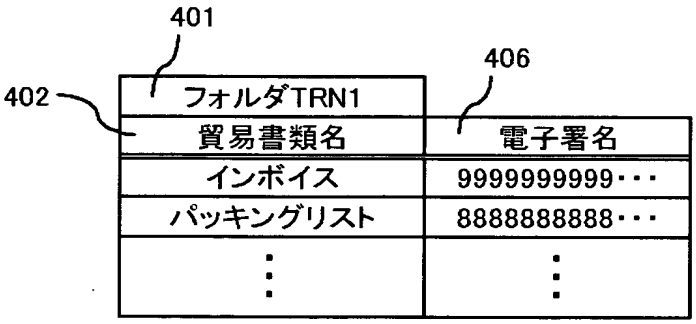
301 フォルダTRN1	
302 貿易書類名	303 ハッシュ値
インボイス	4444444444・・・
パッキングリスト	3333333333・・・
⋮	⋮

【図４】

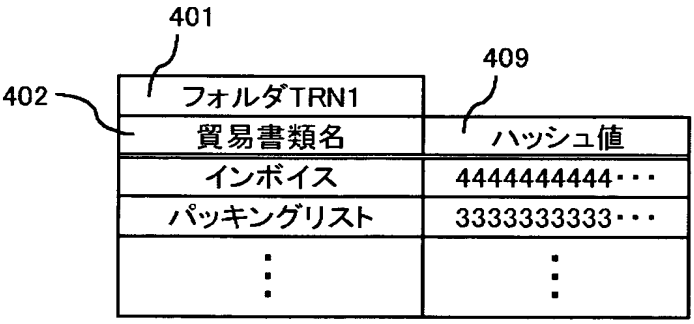
(a)


401
403
402
フォルダTRN1
貿易書類名
貿易書類の属性情報と内容
インボイス
xxxx, xxxxxxxx, xxxxxxxx, xxx, xxxxx, x, xx
パッキングリスト
yyyy, yyyyyyyy, yyyyyyyy, yyy, yyyyy, y, yy

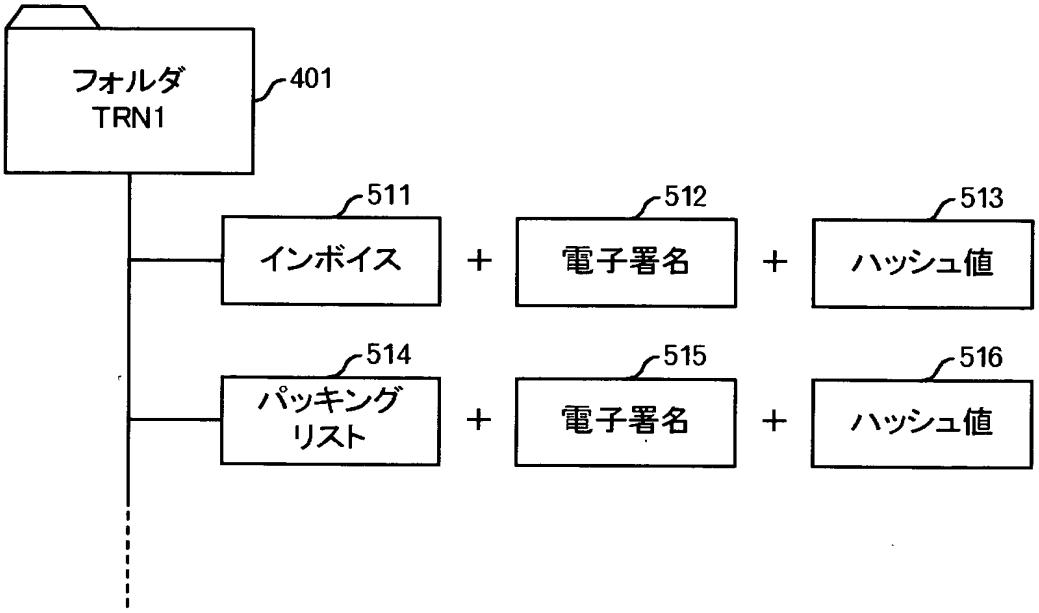
(b)


401
406
402
フォルダTRN1
貿易書類名
電子署名
インボイス
9999999999･･･
パッキングリスト
8888888888･･･

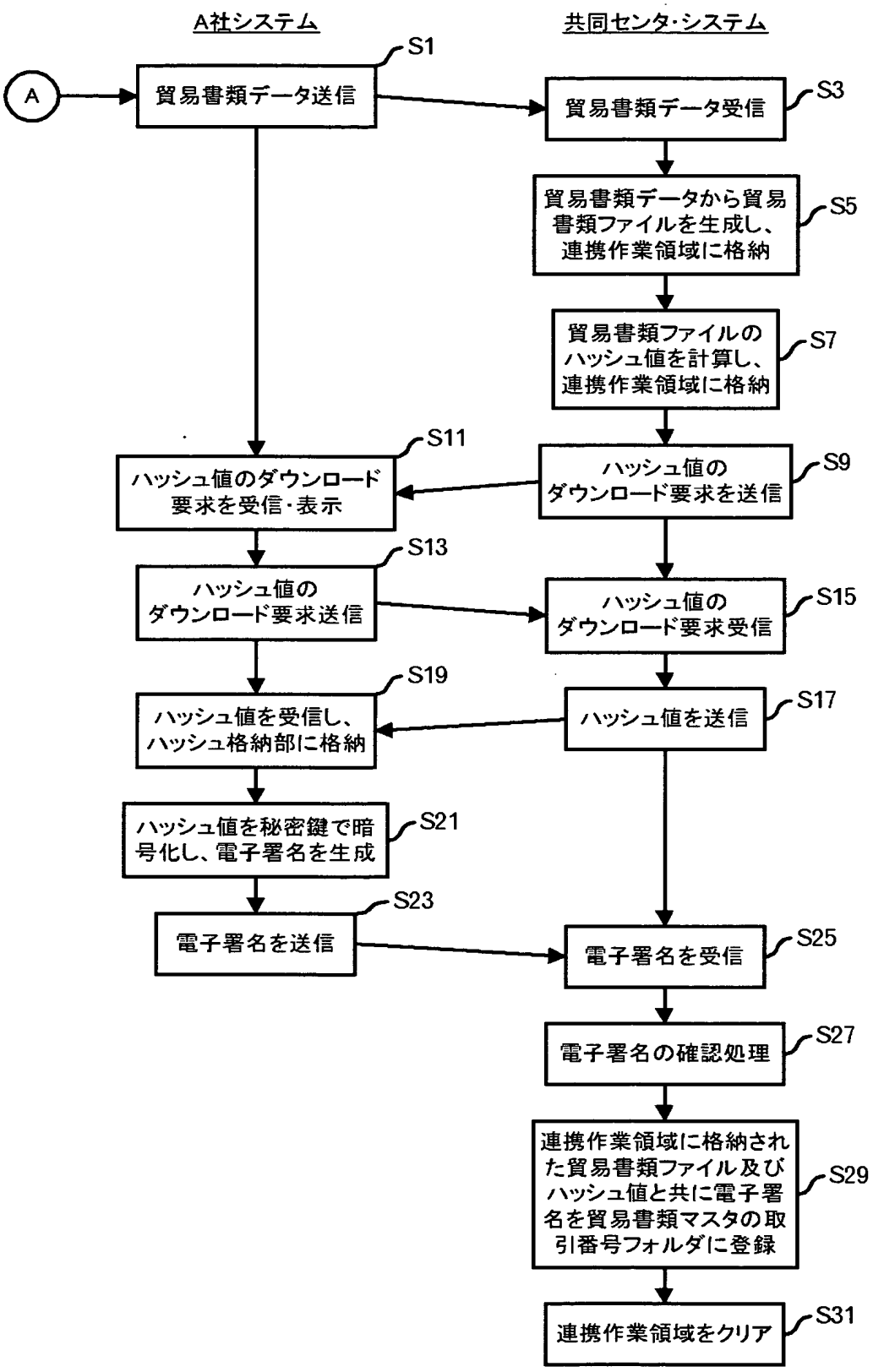
(c)


401
409
402
フォルダTRN1
貿易書類名
ハッシュ値
インボイス
4444444444･･･
パッキングリスト
3333333333･･･

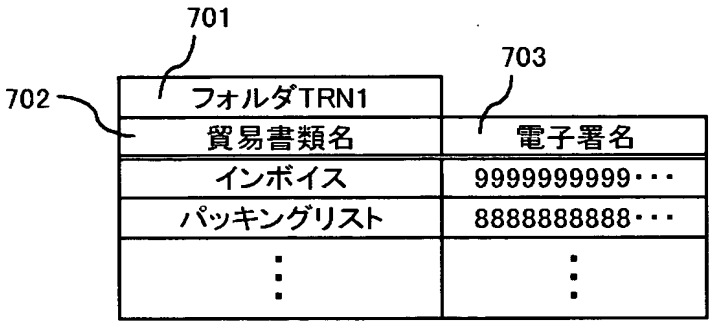
【図５】


フォルダ
TRN1
401
511
インボイス
+
512
電子署名
+
513
ハッシュ値
514
パッキング
リスト
+
515
電子署名
+
516
ハッシュ値

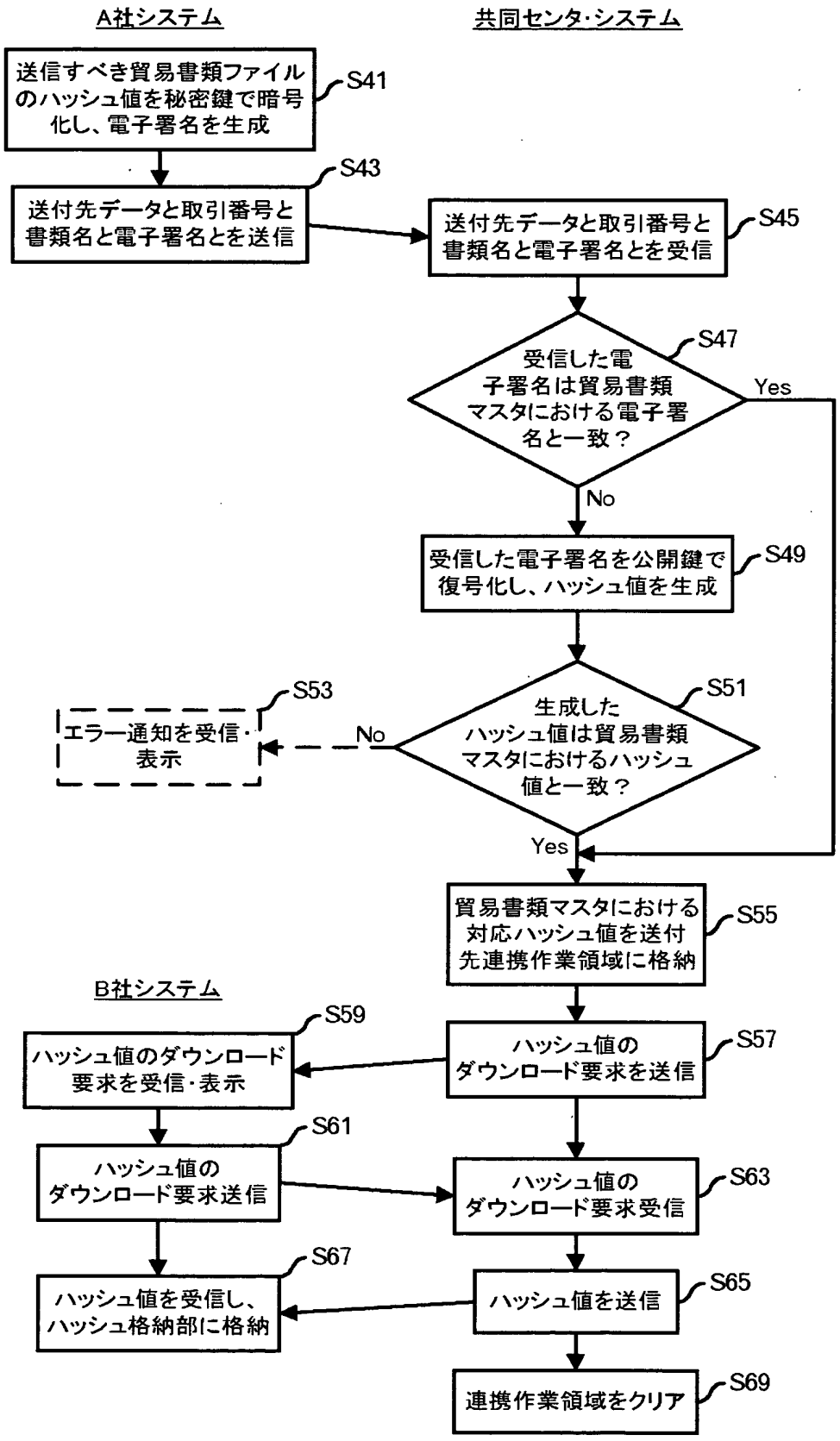
【図６】


A社システム
共同センタ・システム
A
S1
貿易書類データ送信
S3
貿易書類データ受信
S5
貿易書類データから貿易書類ファイルを生成し、連携作業領域に格納
S7
貿易書類ファイルのハッシュ値を計算し、連携作業領域に格納
S9
ハッシュ値のダウンロード要求を送信
S11
ハッシュ値のダウンロード要求を受信・表示
S13
ハッシュ値のダウンロード要求送信
S15
ハッシュ値のダウンロード要求受信
S17
ハッシュ値を送信
S19
ハッシュ値を受信し、ハッシュ格納部に格納
S21
ハッシュ値を秘密鍵で暗号化し、電子署名を生成
S23
電子署名を送信
S25
電子署名を受信
S27
電子署名の確認処理
S29
連携作業領域に格納された貿易書類ファイル及びハッシュ値と共に電子署名を貿易書類マスタの取引番号フォルダに登録
S31
連携作業領域をクリア

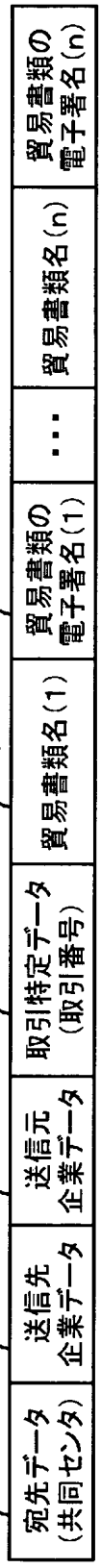
【図７】


701
703
702
フォルダTRN1
貿易書類名
電子署名
インボイス
9999999999・・・
パッキングリスト
8888888888・・・

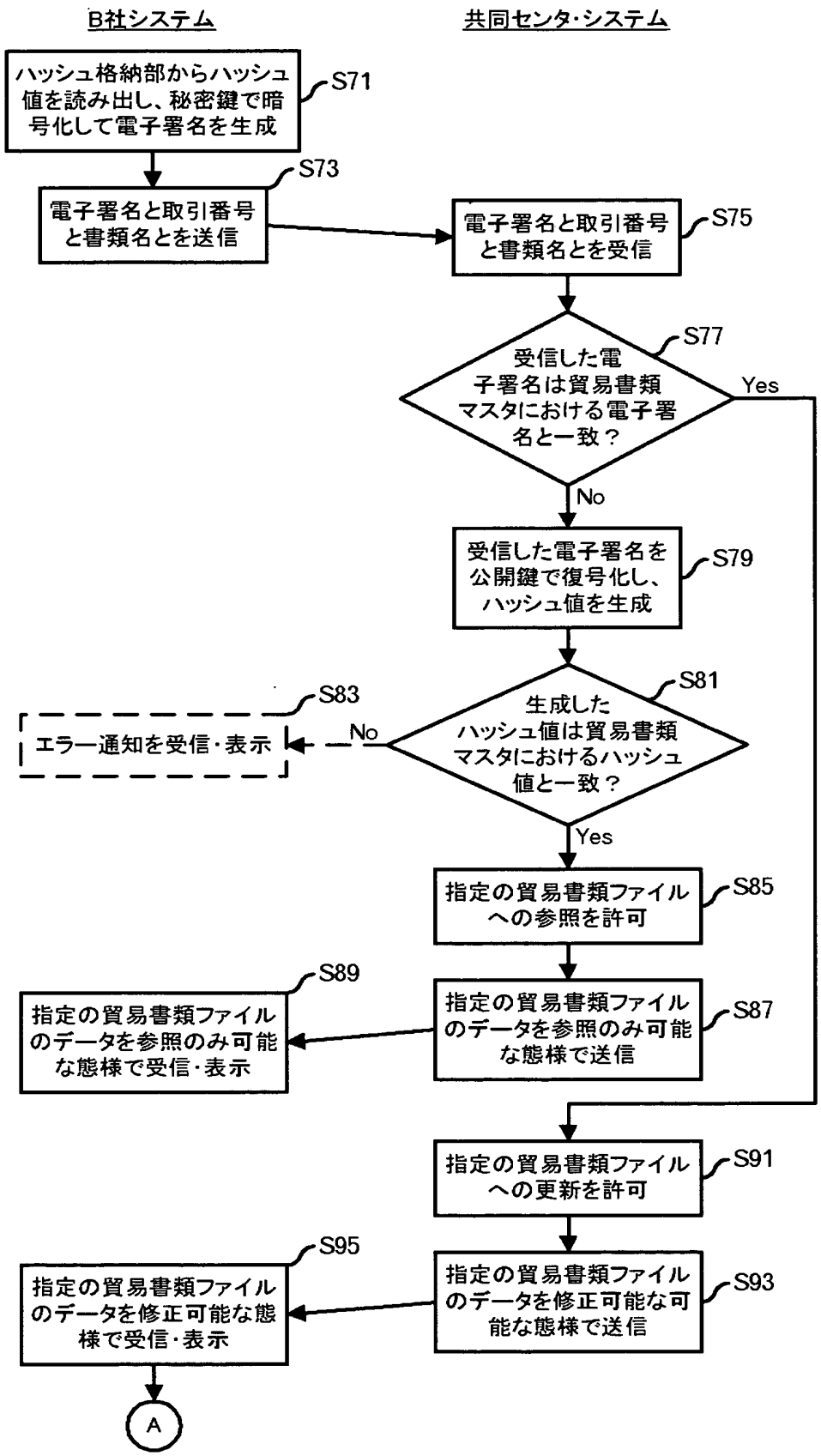
【図８】


A社システム
共同センタ･システム
送信すべき貿易書類ファイルのハッシュ値を秘密鍵で暗号化し、電子署名を生成
S41
S43
送付先データと取引番号と書類名と電子署名とを送信
送付先データと取引番号と書類名と電子署名とを受信
S45
受信した電子署名は貿易書類マスタにおける電子署名と一致？
S47
Yes
No
受信した電子署名を公開鍵で復号化し、ハッシュ値を生成
S49
生成したハッシュ値は貿易書類マスタにおけるハッシュ値と一致？
S51
No
エラー通知を受信･表示
S53
Yes
貿易書類マスタにおける対応ハッシュ値を送付先連携作業領域に格納
S55
B社システム
ハッシュ値のダウンロード要求を受信･表示
S59
ハッシュ値のダウンロード要求を送信
S57
ハッシュ値のダウンロード要求送信
S61
ハッシュ値のダウンロード要求受信
S63
ハッシュ値を受信し、ハッシュ格納部に格納
S67
ハッシュ値を送信
S65
連携作業領域をクリア
S69

【図９】


901
宛先データ
(共同センタ)
902
送信先
企業データ
903
送信元
企業データ
904
取引特定データ
(取引番号)
905
貿易書類名(1)
906
貿易書類の
電子署名(1)
・・・
貿易書類名(n)
貿易書類の
電子署名(n)

【図１０】


B社システム
共同センタ・システム
ハッシュ格納部からハッシュ値を読み出し、秘密鍵で暗号化して電子署名を生成
S71
S73
電子署名と取引番号と書類名とを送信
電子署名と取引番号と書類名とを受信
S75
S77
受信した電子署名は貿易書類マスタにおける電子署名と一致？
Yes
No
受信した電子署名を公開鍵で復号化し、ハッシュ値を生成
S79
S81
生成したハッシュ値は貿易書類マスタにおけるハッシュ値と一致？
No
S83
エラー通知を受信・表示
Yes
指定の貿易書類ファイルへの参照を許可
S85
S89
指定の貿易書類ファイルのデータを参照のみ可能な態様で受信・表示
指定の貿易書類ファイルのデータを参照のみ可能な態様で送信
S87
指定の貿易書類ファイルへの更新を許可
S91
S95
指定の貿易書類ファイルのデータを修正可能な態様で受信・表示
指定の貿易書類ファイルのデータを修正可能な可能な態様で送信
S93
A

【図１１】


1101
宛先データ（共同センタ）
1102
送信元企業データ
1103
取引特定データ（取引番号）
1104
貿易書類名(1)
1105
貿易書類の電子署名(1)
・・・
貿易書類名(n)
貿易書類の電子署名(n)

【書類名】　　要約書

【要約】

【課題】

暗号化技術を用いたアクセス制御を可能にする。

【解決手段】

特定のデータに対する第1の電子署名をユーザの端末から受信するステップと、受信した第1の電子署名と特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較するステップと、第1の電子署名と第2の電子署名とが一致すると判断された場合には、ユーザに対して特定のデータの更新権限を付与する設定を行うステップと、第1の電子署名と第2の電子署名とが一致しないと判断された場合には、第1の電子署名から第1のハッシュ・データを生成し、記憶装置に格納するステップと、第1のハッシュ・データと特定のデータに対応してデータ登録部に登録された第2のハッシュ・データとを比較するステップと、第1のハッシュ・データと第2のハッシュ・データとが一致すると判断された場合には、ユーザに対して特定のデータの閲覧権限を付与する設定を行うステップとを含む。

【選択図】　図１

特願２００２－２６９１１５

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　神奈川県川崎市中原区上小田中１０１５番地
氏　名　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社